

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



ZPP.271.2.2.2025

Załącznik nr 5 do SWZ

## **OPIS PRZEDMIOTU ZAMÓWIENIA**

### **Zadanie obejmuje:**

- 1) Dostawę i wdrożenie programu do zarządzania i monitorowania komputerami w Urzędzie Gminy Lubichowo wraz ze szkoleniem administratora sieci użytkownika;
- 2) Dostawę i wdrożenie systemu Kontroli dostępu do sieci (NAC) w Urzędzie Gminy Lubichowo wraz ze szkoleniem administratora sieci użytkownika;
- 3) Dostawę i wdrożenie system backupu w Urzędzie Gminy Lubichowo wraz ze szkoleniem administratora sieci użytkownika;
- 4) Dostawę i wdrożenie zarządzalnych przełączników sieciowych (TYP 1 i TYP 2) w Urzędzie Gminy Lubichowo wraz ze szkoleniem administratora sieci użytkownika;
- 5) Dostawę i wdrożenie sieci bezprzewodowej w Urzędzie Gminy Lubichowo wraz ze szkoleniem administratora sieci użytkownika;
- 6) Dostawę zasilaczy UPS dla stacji komputerowych w Urzędzie Gminy Lubichowo;
- 7) Dostawę zasilaczy UPS dla sprzętu serwerowego w Urzędzie Gminy Lubichowo;
- 8) Dostawę i wdrożenie urządzeń UTM (TYP 1 i TYP 2) w Publicznej Szkole Podstawowej w Lubichowie im. Ks. Kard. Stefana Wyszyńskiego oraz Publicznej Szkole Podstawowej w Zelgoszczy wraz ze szkoleniem administratora sieci użytkownika;
- 9) Dostawę Platformy szkoleniowej dla użytkowników Urzędzie Gminy Lubichowo, Publicznej Szkole Podstawowej w Lubichowie im. Ks. Kard. Stefana Wyszyńskiego oraz Publicznej Szkole Podstawowej w Zelgoszczy;
- 10) Specjalistyczne szkolenia z zakresu cyberbezpieczeństwa IT.

### **Wykonawca jest zobowiązany do realizacji przedmiotu zamówienia przy udziale osoby (lub osób) posiadającej:**

- posiadającej certyfikat specjalisty (minimum 2 poziom certyfikacji) wydany przez producenta zaoferowanego systemu backup i posiadającą wiedzę z zakresu instalacji, konfigurowania oraz zarządzania oferowanym systemem backupu,
- posiadającej certyfikat inżyniera systemu kontroli dostępu do sieci (NAC), wydany przez producenta lub autoryzowaną instytucję certyfikującą, w zakresie instalacji, konfiguracji oraz wsparcia serwisowego

### **Wymaganie minimalne dla poszczególnych pozycji.**

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



**Ad. 1 System do zarządzania i monitorowania komputerami.**

**1. Architektura / budowa**

- 1.1. System musi umożliwić bezproblemową i stabilną obsługę co najmniej 30 Klientów jednocześnie.
- 1.2. Błąd: nie znaleziono źródła odwołania:
  - 1.2.1. Klient – komponent odpowiedzialny za zarządzanie komputerem, zbieranie danych oraz przysyłanie danych do serwera z wykorzystaniem bezpiecznego połączenia, pracujący w trybie usługi systemowej.
  - 1.2.2. Konsola administracyjna – przeznaczona do zarządzania całym systemem, w formie w pełni funkcjonalnej aplikacji internetowej (webowej).
  - 1.2.3. Panel pracownika – aplikacja webowa, niewymagająca dodatkowego logowania, dostępna dla pracowników, udostępniająca wybrane dane z konsoli administracyjnej oraz pozwalająca na interakcję z pracownikiem w wybranych obszarach.
  - 1.2.4. Serwer – oprogramowanie odpowiadające za utrzymywanie komunikacji i wymianę danych z Klientami.
  - 1.2.5. Baza danych pracująca na silniku Microsoft SQL Server w wersjach wyspecyfikowanych poniżej.
- 1.3. Konfiguracja Architektury:
  - 1.3.1. Komponenty systemu (Klient, konsola administracyjna, serwer, baza danych) aktualizują się automatycznie poprzez bezpieczne połączenie.
  - 1.3.2. System zawiera mechanizmy automatycznej konserwacji zgodnie z harmonogramem.

**2. Wymagania systemowe**

- 2.1. Konsola administracyjna musi działać w pełni responsywnie (niezależnie od wielkości i rozdzielczości ekranu urządzenia wyświetlającego) na dowolnej przeglądarce stron WWW zgodnej z HTML5 (np. Internet Explorer 11, FireFox, Chrome, Opera).
- 2.2. Klient musi działać na systemach 32 i 64 bitowych: Windows Server 2012/2012R2/2016/2019/2022, Windows 7/8/8.1/10/11, MacOS 10.7/10.8, Linux dla wersji: Ubuntu v.11.04 lub wyższa, Debian v.6.0 lub wyższa, RedHat v.6.0 lub wyższa, CentOS v.6.0 lub wyższa, Fedora v.16 lub wyższa.
  - 2.2.1. Klient wspiera poniższe przeglądarki internetowe w zakresie monitorowania aktywności użytkownika w sieci: Opera wersja 63.0.3368.94, Chrome wersja 77.0.3865.90, FireFox wersja 69.0.2
- 2.3. Serwer musi działać na systemach 64 bitowych: Windows Server 2016/2019/2022, Windows 7/8/8.1/10/11.
- 2.4. Serwer www musi być oparty o platformę Microsoft 64 bit (Windows Server 2016/2019/2022, Windows 10 oraz Java 8 (JRE lub JDK), Apache Tomcat 9.
- 2.5. Baza danych musi działać na silniku Microsoft SQL Server 2014/2016/2017/2019/2022 w wersji 64 bitowych bezpłatnym (np. Microsoft SQL Server Express Edition).
- 2.6. System musi mieć możliwość pracy w środowisku wirtualnym Microsoft Hyper-V oraz VMWare.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

### 3. Interfejsy

- 3.1. System musi umożliwiać wielokrotny, zgodny z harmonogramem lub na życzenie, import użytkowników, komputerów, struktury organizacyjnej (całości bądź wybranego kontenera) z usługi MS Active Directory, przy czym import struktury organizacyjnej musi następować we wskazane miejsce struktury organizacyjnej zdefiniowanej w systemie.
- 3.2. System musi umożliwiać import danych z CSV, Excel, Microsoft SQL Server, MySQL, PostgreSQL
- 3.3. System zapewnia integrację z modelem LLM.

### 4. Funkcjonalności systemu zarządzania infrastrukturą IT

#### 4.1. Funkcjonalność Klienta

- 4.1.1. System musi umożliwiać pełne zdalne zarządzanie Klientami, obejmujące uruchamianie i wyłączanie, zmianę konfiguracji Klienta, inicjowanie skanowania oraz wykonanie poleceń systemowych. Klient powinien wyświetlać komunikaty w HTML z dokładnymi danymi o czasie wyświetlenia i użytkownika.

#### 4.2. Funkcjonalność konsoli administracyjnej.

- 4.2.1. Konsola administracyjna musi być wielojęzyczna (polski i angielski) i oferować intuicyjny interfejs z pełnym zestawem funkcji zarządzania (dodawanie, modyfikowanie, usuwanie). Musi także zawierać co najmniej 140 różnorodnych dashboardów, w tym dashboardy użytkownika, prezentujące parametry infrastruktury, sieci oraz bezpieczeństwa. Użytkownicy powinni mieć możliwość samodzielnego konfigurowania dashboardów użytkownika, a dashboardy sieciowe i bezpieczeństwa muszą zawierać szczegółowe widżety z informacjami o stanie usług i bezpieczeństwie.

- 4.2.2. W konsoli powinna istnieć funkcja filtrowania danych na dashboardach oraz możliwość personalizacji interfejsu przez użytkownika, w tym definiowanie własnych pól, filtrów i widoków, z zachowaniem tych ustawień pomiędzy sesjami. Konsola musi także umożliwiać definiowanie poziomów uprawnień dla użytkowników i grup, z opcją dziedziczenia oraz integrację z Active Directory dla zarządzania dostępem.

- 4.2.3. Konsola powinna posiadać zaawansowane funkcje zarządzania rekordami, w tym wykonanie poleceń na wielu rekordach jednocześnie oraz dostęp do szczegółowych informacji o pracy urządzeń.

#### 4.3. Funkcjonalność panelu pracownika

- 4.3.1. Panel pracownika systemu musi automatycznie uruchamiać się i autoryzować przy logowaniu użytkownika, z możliwością definiowania zakresu dostępnych informacji przez administratora dla poszczególnych grup pracowników. Panel kierownika powinien dodatkowo agregować i analizować dane z paneli pracowników. Informacje w panelu muszą być organizowane w logiczne sekcje, które można indywidualnie lub grupowo włączać i wyłączać przez administratora.

#### 4.4. Zarządzanie licencjami

- 4.4.1. System musi umożliwiać kompleksowe zarządzanie licencjami w różnych modelach i strukturach organizacyjnych, w tym audyty, zarządzanie oprogramowaniem i oprogramowaniem zabronionym, oraz przypisywanie i rozliczanie różnych typów licencji. Musi także rejestrować historię licencji oraz zapewniać funkcje inwentaryzacji i zdalnej dezinstalacji oprogramowania.

#### 4.5. Wzorce aplikacji i pakietów

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

- 4.5.1. System powinien posiadać rozbudowaną bazę wzorców oprogramowania, umożliwiać definiowanie własnych wzorców i automatycznie importować nowe wzorce od producenta. Musi także dostarczać szczegółowe informacje o zainstalowanych pakietach i ich wykorzystaniu, w tym edycje Microsoft Office.
- 4.6. Inwentaryzacja sprzętu komputerowego i urządzeń.
  - 4.6.1. System musi oferować rozbudowane funkcje inwentaryzacji sprzętu komputerowego, włączając automatyczną inwentaryzację zarówno w sieci lokalnej jak i zdalnej, szczegółowe skanowanie komponentów (np. RAM, monitory, dyski twarde) oraz zarządzanie informacjami o zainstalowanym sprzęcie. Powinien także umożliwiać ewidencję zmian konfiguracji sprzętu, identyfikować i klasyfikować urządzenia podłączane do komputerów oraz monitorować historię ich podłączeń.
- 4.7. Inwentaryzacja urządzeń sieciowych.
  - 4.7.1. System musi posiadać zdolności do identyfikacji urządzeniami sieciowymi. Wymagane jest posiadanie skanera sieci i SNMP, które automatycznie zbierają dane, analizują jakość połączeń i identyfikują urządzenia na sieci. System powinien także umożliwiać zdalną instalację Klientów i generowanie map sieci.
- 4.8. Inwentaryzacja sprzętu.
  - 4.8.1. System musi umożliwiać wszechstronną inwentaryzację sprzętu, włączając urządzenia inne niż komputery (np. drukarki, routery). Musi zapewniać zarządzanie dokumentacją związaną z urządzeniami, monitorować ich ruch oraz przypominać o terminach gwarancji i umowach utrzymaniowych.
- 4.9. Ochrona danych (DLP)
  - 4.9.1. Ochrona danych (DLP) musi obejmować automatyczne tworzenie listy podłączanych do komputerów urządzeń USB i ich klasyfikację. System powinien dostarczać informacje o historii użytkowania urządzeń zewnętrznych oraz umożliwiać zarządzanie dozwoleńmi do użytku urządzeniami USB zgodnie z zdefiniowanymi regułami.
- 4.10. Zdalna administracja komputerami
  - 4.10.1. System musi oferować kompleksową zdalną administrację komputerami, włączając w to automatyczne wykonywanie dowolnych poleceń (np. zarządzanie aplikacjami, plikami, rejestrami systemowymi) oraz zarządzanie cyklicznymi zadaniami z harmonogramem. Powinien obsługiwać technologię Intel vPro dla zdalnej konfiguracji i zarządzania, a także pozwalać na zdalne przejęcie kontroli nad komputerem za pomocą technologii Ultra VNC, umożliwiając operowanie na wielu sesjach jednocześnie. System powinien integrować zaawansowane mechanizmy skryptowe wspierane przez AI dla automatycznego generowania poleceń oraz umożliwiać zarządzanie i tworzenie zadań cyklicznych z różnorodnymi opcjami cykliczności i zakończenia.
- 4.11. System musi zezwalać na wykonywanie zapytań WMI bez zdalnego połączenia do urządzenia.
- 4.12. System musi zezwalać na edycję rejestrów urządzenia bez wykorzystania zdalnego połączenia pulpitu.
- 4.13. Zdalne Zarządzanie Zaporą (Firewall)
  - 4.13.1. System musi umożliwiać zdalne zarządzanie zaporą sieciową (firewall) globalnie w infrastrukturze, co obejmuje monitorowanie jej stanu w czasie rzeczywistym, definiowanie złożonych zasad zapory z centralnego panelu administracyjnego oraz szybkie identyfikowanie i reagowanie na potencjalne zagrożenia sieciowe.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



#### 4.14. Automatyzacja

4.14.1. System musi oferować możliwość ustalania harmonogramu dla czynności konserwacyjnych, naprawczych i porządkujących, z opcją ustalania częstotliwości i parametrów wejściowych dla każdej czynności oraz możliwością ich zatrzymania lub uruchomienia. Dodatkowo, system musi posiadać mechanizmy automatyzacji takie jak wykonywanie kopii bezpieczeństwa, identyfikacja aplikacji i pakietów, porządkowanie bazy danych oraz usuwanie nadmiarowych danych. System również powinien wysyłać alerty o zdarzeniach takich jak nowe komputery w bazie danych, braki w licencjach i inne zdarzenia krytyczne dla infrastruktury IT.

#### 4.15. Zarządzanie magazynem IT

4.15.1. System musi umożliwiać efektywne zarządzanie magazynem IT, włączając obsługę dowolnej ilości magazynów w różnych lokalizacjach oraz obsługę dokumentów magazynowych typu PZ, RW, WZ, i inne. System powinien prowadzić ewidencję materiałów w magazynach zgodnie z metodą FIFO. Ponadto, system powinien umożliwiać automatyczne łączenie dokumentów magazynowych z zasobami systemu oraz zapewniać przegląd wszystkich dokumentów.

#### 4.16. Repozytorium

4.16.1. Konsola administracyjna systemu musi być wyposażona w repozytorium dokumentów dowolnego typu, które umożliwia dodawanie nowych dokumentów, przeszukiwanie. Repozytorium powinno także umożliwiać definiowanie kontenerów na dokumenty, co ułatwia organizację i zarządzanie dokumentacją.

#### 4.17. Kody kreskowe

4.17.1. System musi wspierać obsługę kodów kreskowych jedno i dwuwymiarowych, umożliwiając parametryzację kodu pod względem wielkości i atrybutów graficznych. System powinien umożliwiać podgląd oraz wydruk kodów kreskowych.

#### 4.18. Wysyłanie wiadomości

4.18.1. System musi oferować funkcję komunikatora, umożliwiającą bezpośrednią wymianę wiadomości między użytkownikami a administratorem systemu, w tym inicjowanie czatu przez administratora oraz przechowywanie historii konwersacji. System powinien także umożliwiać wysyłanie jednorazowych wiadomości ALERT oraz tworzenie szablonów wiadomości do regularnego użytku, z opcją konfiguracji terminu, po którym wiadomość wygaśnie. Ponadto, system powinien wspierać szkolenie pracowników za pomocą wiadomości tekstowych z możliwością definiowania treści szkoleniowych i automatycznego ich wysyłania.

#### 4.19. System musi posiadać możliwość eksportu / importu treści.

#### 4.20. Monitorowanie drukarek sieciowych i wydruków

4.20.1. System musi umożliwić monitorowanie i zarządzanie wydrukami z dowolnej drukarki (lokalnej czy sieciowej), rejestrując szczegółowe informacje o każdym wydruku, w tym koszty, dzięki wbudowanemu cennikowi. System powinien również prognozować przyszłe koszty drukowania oraz pozwalać na zarządzanie drukarkami według różnych parametrów, w tym statusu i materiałów eksploatacyjnych.

#### 4.21. Monitorowanie stron www

4.21.1. System musi oferować monitorowanie aktywności internetowej użytkowników na różnych przeglądarkach, nawet przy szyfrowanych połączeniach (https), rejestrując detale takie jak adresy IP, czas połączenia, a także analizując treści stron za pomocą algorytmów sztucznej inteligencji do klasyfikacji i kontroli treści.

#### 4.22. Monitorowanie serwerów WWW

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

- 4.22.1. System musi zapewniać monitorowanie wybranych serwerów WWW, prezentując informacje o ich statusie i aktywności, umożliwiając analizę treści stron oraz graficzną prezentację danych związanych z ich działaniem, w tym czasem odpowiedzi i aktywnością w określonym okresie.
- 4.23. Monitorowanie dziennika zdarzeń
  - 4.23.1. System musi posiadać zdolność do monitorowania dziennika zdarzeń komputerów, umożliwiając definiowanie i filtrowanie zdarzeń według różnych kategorii.
- 4.24. System musi umożliwiać monitorowanie komunikatów Syslog.
- 4.25. Monitorowanie pracy komputerów
  - 4.25.1. System musi oferować monitorowanie pracy komputerów, w tym dat startu i zakończenia pracy, logowania użytkowników, a także zdalne monitorowanie sesji połączeń, rejestrując szczegóły takie jak adresy IP i dane użytkowników.
- 4.26. Monitorowanie sensorów
  - 4.26.1. System musi integrować monitoring warunków środowiskowych za pomocą sensorów po SNMP, umożliwiając graficzną prezentację danych, wysyłanie alertów.
- 4.27. Repozytorium CMDB
  - 4.27.1. System musi posiadać zintegrowane repozytorium CMDB, umożliwiające zarządzanie zasobami IT, w tym szczegółowe informacje o użytkownikach, urządzeniach, licencjach, a także o oprogramowaniu i jego licencjach, z możliwością importu i eksportu danych.
- 4.28. Worktime manager
  - 4.28.1. System musi umożliwiać monitorowanie i analizę czasu pracy użytkowników, z możliwością definiowania grup przypisanych do przełożonych i prezentacji szczegółowych danych o aktywności użytkowników w formie widżetów i danych analitycznych. Informacje o czasie pracy, sesjach, aktywności w aplikacjach oraz produktywności powinny być możliwe do udostępnienia w panelu pracownika.
- 4.29. Raportowanie i eksport danych
  - 4.29.1. System musi oferować zaawansowane możliwości raportowania i eksportu danych, umożliwiając wyeksportowanie informacji do różnych formatów, w tym xls, csv, html, oraz graficznych. Powinien także wspierać generowanie wieloparametrycznych raportów z możliwością stosowania filtrów, obsługę wieloinstancyjności raportowania oraz integrację z narzędziami do tworzenia raportów takimi jak SAP Crystal Reports i Stimulsoft, obejmując co najmniej 150 zdefiniowanych raportów. Dodatkowo, system musi posiadać możliwość konfiguracji harmonogramu umożliwiającego cykliczne wysyłanie raportów oraz zapisywanie ich w dowolnym miejscu, z automatycznym generowaniem raportu w formacie PDF jako wynikiem wykonania harmonogramu.
- 4.30. System musi zapewnić interfejs API.
  - 4.30.1. System musi oferować rozbudowany interfejs API, umożliwiający komunikację za pomocą REST API. Musi on zapewniać szyfrowaną komunikację z użyciem protokołu TLS 1.3 oraz możliwość tworzenia złożonych requestów JSON. Klucze zabezpieczeń powinny być modyfikowalne i mogą mieć co najmniej 32 znaki.
- 4.31. Powiadomienia
  - 4.31.1. System musi umożliwiać generowanie różnorodnych powiadomień, w tym alertów w konsoli, e-maili oraz wiadomości SMS, z możliwością edycji treści powiadomień i definiowania grup odbiorców. Powinien obsługiwać automatyczne wywoływanie

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

zadań i integrować się z CMD oraz Windows PowerShell, zapewniając co najmniej 30 predefiniowanych powiadomień oraz możliwość ich personalizacji.

**4.32. Bezpieczeństwo**

4.32.1. System musi zapewniać rozbudowane funkcje bezpieczeństwa, w tym definicję i zarządzanie prawami dostępu oraz zaawansowane opcje uwierzytelniania. Wymaga silnych haseł, obsługuje wieloskładnikowe uwierzytelnianie i posiada mechanizmy szyfrowania danych.

**5. Wsparcie i pomoc**

**5.1.1. Pomoc techniczna**

5.1.1.1. Musi być świadczona co najmniej w dni robocze w godzinach od 8.00-16.00.

5.1.1.2. Utrzymaniem Oprogramowania jest zapewnienie aktualizacji Oprogramowania (asysta techniczna) oraz nieprzerwanego działania Oprogramowania (usługi SLA), jak również zapewnienie świadczenia innych usług wspomagających korzystanie z Oprogramowania.

5.1.1.3. Wykonawca przeprowadzi szkolenie administratorów sieci użytkownika w zakresie niezbędnym do poprawnego zarządzania systemem.

5.1.1.4. Czas trwania usługi SLA wynosi minimum 12 miesięcy od dnia dostawy

5.1.1.5. Jeżeli niezbędne, Wykonawca zapewni potrzebną platformę sprzętową wraz z licencjami systemowymi, pozwalającymi na wdrożenie systemu zarządzania i monitorowania komputerami.

**Ad. 2 System kontroli dostępu do sieci NAC**

**Zakres obejmuje:**

- a) zakup systemu zarządzania dostępem do sieci komputerowej typu NAC (Network Access Control) wraz z wsparciem technicznym,
- b) usługi informatycznych w zakresie wdrożenia wyżej wymienionego sprzętu i oprogramowania,
- a) szkolenie stacjonarne dla pracowników urzędu w zakresie obsługi systemu NAC.

Zaoferowane przez Wykonawcę sprzęt i oprogramowanie muszą spełniać minimalne wymagania oraz zostać dostarczony na warunkach określonych poniżej.

**Podstawowa funkcjonalność systemu NAC:**

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji.
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

7. System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 500 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
  - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x
  - Maszyny fizyczne - serwery wspierane przez producenta.
11. System musi posiadać funkcjonalność serwerów:
  - serwera RADIUS dla infrastruktury sieciowej,
  - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
  - serwera SYSLOG,
  - serwera TACACS+,
  - serwera Monitoring,
  - serwera DHCP,
  - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
  - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now).
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
- Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
  - Czy włączony jest firewall
  - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
  - Czy jest włączone szyfrowanie dysku systemowego
  - Czy urządzenie końcowe jest połączone do domeny Microsoft Active Directory
  - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
  - Czy w systemie są uruchomione procesy wskazane przez administratora
  - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
  - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
    - Wartości klucza rejestru
    - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratorzy sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
- Microsoft Windows
  - Mac OS
  - iOS
  - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratorzy sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

### **Mechanizmy uwierzytelniania**

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
  - MAC,
  - PAP/ASCII,
  - CHAP,
  - SNMP,
  - 802.1X.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.

3. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
4. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
5. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
6. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
  - Tożsamość/Urządzenie końcowe,
  - Grupa tożsamości/urządzeń końcowych,
  - Parametry urządzeń końcowych, min: system operacyjny, wersja,
  - Atrybuty Active Directory,
  - Jednostka organizacyjna tożsamości/urządzeń końcowych,
  - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
  - Grupy urządzeń sieciowych,
  - Porty urządzeń sieciowych,
  - Grupy portów urządzeń sieciowych,
  - Jednostka organizacyjna portów,
  - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
  - Data, czas ważności polityki,
  - Wewnętrzny Captive Portal,
  - Metoda autoryzacji.
7. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
8. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
9. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
10. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
11. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
12. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
14. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



15. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
16. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
17. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
18. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
19. System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

#### **Obsługa serwerów certyfikatów CA**

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
  - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
  - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
  - Możliwość generowania certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
  - usługę OCSP (Online Certificate Status Protocol).

#### **Obsługa serwerów DHCP**

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
  - Uruchamianie usługi dla wybranych podsieci,
  - Przypisanie ustalonego adresu IP dla adresu MAC.
  - Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
  - Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
  - Możliwość określania braku dostępu dla wybranych adresów MAC,
  - Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
  - Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
  - Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
  - Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



- Dokonywanie zmian bez konieczności wyłączenia usług.

### **Obsługa serwerów TACACS+**

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

### **Raportowanie i monitoring**

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.
11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
  - Logowania, wylogowania z system w tym błędne logowania
  - Logowania do sieci 802.1X

### **Alarmy**

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
  - wiadomości e-mail,
  - Syslog,
  - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
  - Ilości obsługiwanych transakcji RADIUS,
  - Opóźnienie obsługi transakcji RADIUS,
  - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
  - badanie łączności IP za pomocą ping, traceroute,
  - tcpdump protokołów RADIUS, TACACS+,
  - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
    - nazwy użytkownika,
    - adresu MAC,
    - statusu uwierzytelnienia (udana lub nieudana),
    - powodu, jeżeli uwierzytelnienie nieudane,
    - zakresu czasowego, co do dnia, godziny i minuty,
  - wykonanie zdalnego polecenia na urządzeniu sieciowym.

### **Wymagania dotyczące wdrożenia i harmonogram ramowy:**

- Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta.
- Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA).
- Konfiguracja urządzenia firewall (dodatknie VLAN-u gościnnego, ustawienie polityk, etc.).
- Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list).
- Integracja istniejących (UTM Stormshield SN 310, SN310A28B5466B7 firmware: 3.7.20, pozostałych urządzeń wskazanych przez zamawiającego) oraz dostarczanych urządzeń

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



sieciowych (switche, AP WiFi) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach.

- Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy.
- Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy.
- Przeprowadzenie szkolenia dla administratorów z konfiguracji i administrowania Systemem NAC. Dwudniowe szkolenie online zdalne dla do 2 osób po 6h dziennie.
- Przygotowanie dokumentacji powykonawczej opisującej wykonane prace oraz sposób konfiguracji poszczególnych urządzeń do 14 dni po zakończeniu wdrożenia.
- Jeżeli niezbędne, Wykonawca zapewni potrzebną platformę sprzętową wraz z licencjami systemowymi, pozwalającymi na wdrożenie systemu zarządzania i monitorowania komputerami.

**Szkolenia/warsztaty:**

- Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC.
- Warsztaty zostaną przeprowadzone dla maks. 2 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC.
- Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
- Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.

**Licencja wsparcia technicznego producenta oprogramowania:**

Wykonawca dostarczy dożywotnią licencję systemu NAC wraz z min. 12 miesięczną licencją na wsparcie producenta oprogramowania

Licencja ta powinna obejmować minimum:

- Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC.
- Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia.
- Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów.
- Dostęp do dokumentacji i instrukcji na stronie internetowej.
- Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania.

**Ad. 3. System Backupu.**

Zakres obejmuje:

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



1. dostawę i wdrożenie dedykowanej macierzy do backupu wraz z oprogramowaniem w siedzibie Urzędu Gminy w Lubichowie,
2. wykonanie odmiejszczenia backupu Urzędu Gminy w Lubichowie i wyniesienie do lokalizacji Przedszkola Publicznego, ul. Zblewska 30,
3. usługi przedwdrożeniowe i wdrożenie.

Zamawiający wymaga dostarczenia i wdrożenia macierzy do backupu z dedykowanym oprogramowaniem oraz infrastrukturą sieciową, niezbędną do wykonania odmiejszczenia backupu na urządzeniu klasy NAS będącego własnością Zamawiającego (QNAP TS-832PXU).

Wymagania minimalne dla macierzy do backupu z dedykowanym oprogramowaniem (dostawa i wdrożenie obejmują 1 komplet):

#### Zarządzanie i magazyny

1. Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024r.
2. System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.
3. Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
  - a. Obudowa typu Cube Desktop
  - b. Procesor Intel i3 12th gen
  - c. Pamięć RAM 16GB
  - d. Przestrzeń dostępna na przechowywanie danych 8TB
  - e. Osobny dysk systemowy NVME 256 GB
  - f. Interfejs sieciowy 1Gb Ethernet
  - g. Gwarancja o czasie trwania analogicznym do trwania wsparcia technicznego.
4. Produkt dostępny w polskiej wersji językowej.
5. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej.
6. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków.
7. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów.
8. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych.
9. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT.
10. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft.
11. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe.
12. System zarządzania nie może być oparty o relacyjne bazy danych.
13. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
14. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



15. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
16. Rozwiązanie musi być systemem multistorage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
17. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
18. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
19. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
20. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
21. Rozwiązanie zapewnia backup jednorzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
22. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
23. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych.
24. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
25. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
26. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).
27. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
28. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
29. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika.
30. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
31. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z niniejszym opisem przedmiotu zamówienia

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



32. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
33. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
34. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
35. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych.
36. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
37. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
38. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
39. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
40. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
41. System musi pozwalać na automatyczne aktualizacje oprogramowania.
42. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
43. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS i innych środowiskach w celu ich zabezpieczenia.
44. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
45. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
46. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
47. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
48. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
49. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
50. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



- dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
51. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
  52. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
  53. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
  54. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych, min. Custom, Basic, G-F-S, Forever incremental.
  55. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
  56. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3 oraz dedykowana chmura producenta appliance'u.
  57. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole SMB, S3, NFS, iSCSI, katalog lokalny.
  58. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
  59. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniem zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
  60. Możliwość generowania raportów dobowych w oparciu o harmonogram.
  61. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (Data Center powinno być zlokalizowane na terenie Polski).
  62. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna).
  63. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
  64. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienie e-mail. (poziom definiowany indywidualnie dla każdego magazynu).

#### Wspierane systemy

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:

1. Alpine 3.10+,
2. Debian: 9+,
3. Ubuntu: 16.04+,

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



4. Fedora: 29+,
5. CentOS: 7+,
6. RHEL: 6+,
7. openSUSE: 15+,
8. SUSE Enterprise Linux (SLES): 12 SP2+,
9. macOS: 10.13+,
10. Windows: 7, 8.1, 10(1607+),
11. Windows Server: 2008 R2+,

Środowisk wirtualnych:

1. Hyper-V 2016+,
2. VMware: 6.7+.

#### Środowiska fizyczne i bazy danych

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.
3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odtwarzania. Dodatkowo system musi obsługiwać funkcję przyrostowego skalowania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

#### Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowaniem zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.
5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

#### Aplikacje SaaS

1. Ochrona z tej samej konsoli dla Microsoft 365 minimum na poziomie, skrzynek pocztowych, onedrive, kontaktów, kalendarza.
2. Rozwiązanie musi umożliwiać przywracanie danych Microsoft 365: do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst oraz do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji).
3. System musi umożliwiać granularne odtwarzanie danych, tj. pojedynczych plików z kopii obrazu dysku oraz pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.
4. System musi umożliwiać zabezpieczanie środowisk Git, w tym GitHub, GitLab oraz Bitbucket wraz z metadanymi.
5. System musi umożliwiać odtworzenie dowolnego środowiska Git w dowolnym innym środowisku Git, tzw. odtwarzanie crossowe.
6. System musi umożliwiać zabezpieczenie metadanych zebranych wokół repozytorium w ramach zabezpieczanego środowiska Git.
7. System musi umożliwiać odtwarzanie metadanych repozytorium Git do dowolnego innego środowiska Git w przypadku chęci odtworzenia repozytorium.
8. System musi umożliwiać zabezpieczenie środowisk Jira.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



9. System musi umożliwiać odtworzenie środowiska Jira do chmury lub środowiska lokalnego.

#### Licencjonowanie i wsparcie techniczne

1. Wszystkie linie wsparcia muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta przez okres minimum 12 miesięcy od dostawy
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticket-owego oraz wsparcia telefonicznego.
6. W ramach dostawy rozwiązania, dostawca musi wyznaczyć dedykowanego opiekuna technicznego od strony producenta rozwiązania backupowego.
7. W ramach dokumentacji posprzedażowej Dostawca musi dostarczyć bezpośredni numer telefonu oraz adres e-mail do dedykowanego opiekuna technicznego od strony producenta rozwiązania backupowego.
8. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie: nielimitowanej ilości maszyn wirtualnych, nielimitowanej ilości serwerów fizycznych, nielimitowanej ilości stacji roboczych.
9. Licencje musi być dostępna w wersji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu.
10. Licencje powinny umożliwiać korzystanie z mechanizmu replikacji na dowolne zasoby lokalne.
11. Licencja powinna umożliwiać skorzystanie z przestrzeni chmurowej dostarczonej bezpośrednio przed producenta, min. 1,6 TB przez cały okres trwania gwarancji NBD na warstwę sprzętową. Zamawiający w dalszej eksploatacji systemu chciałby mieć możliwość skorzystania poprzez podniesienie poziomu wsparcia u dostawcy rozwiązania, za dodatkową opłatą.

#### Anty-ransomware i bezpieczeństwo

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menadżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu ani żaden inny komponent, którego awaria sparaliżowałaby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.

**2) Wykonanie odmiejszczenia backupu Urzędu Gminy w Lubichowie i wyniesienie go do budynku Przedszkola Publicznego w Lubichowie, ul. Zblewska 30**

Posiadane przez Zamawiającego urządzenie backupu QNAP TS-832PXU wraz z dyskami należy:

- zainstalować w budynku Przedszkola Publicznego w Lubichowie, przy ulicy Zblewskiej 30,
- połączyć z siecią LAN Zamawiającego, z wykorzystaniem dostarczanych również w ramach niniejszego zadania, urządzeń sieciowych o parametrach nie niższych niż opisane poniżej,
- wykonawca będzie zobowiązany dostarczyć wszelki pozostały sprzęt sieciowy, niewyspecyfikowany w zadaniu, a niezbędny do realizacji zadania,
- wdrożyć jako dodatkowe repozytorium zapasowe do urządzenia opisanego w punkcie 1).

Realizowane, dedykowane połączenie do repozytorium zapasowego systemu kopii zapasowych, musi spełniać następujące wymagania:

- MTU min 1504 bajty,
- przepustowość min. 760 Mb/s oraz 1480 kpps dla pakietów o rozmiarze 64 bajtów,
- przepustowość min. 990 Mb/s oraz 340 kpps dla pakietów o rozmiarze 512 bajtów,
- MTBF min. 180 tys. godzin,
- akceleracja sprzętowa protokołu IPSec.

Powyższe urządzenia sieciowe należy dostarczyć wraz z kompletem okablowania, zasilaczy, adapterów i akcesoriów montażowych, zainstalować w lokalizacjach Zamawiającego, uruchomić i przetestować, zgodnie z powyższymi zapisami.

Jeżeli niezbędne będzie wybudowanie niezbędnego medium transmisyjnego, wykona to wykonawca włącznie z infrastrukturą towarzyszącą.

Wykonawca musi również przewidzieć zabezpieczenie wymaganej przestrzeni montażowej, potrzebnej na zainstalowane powyższych urządzeń sieciowych.

**3) Usługi przedwdrożeńowe i wdrożenia.**

W ramach usług wdrożenia Wykonawca wykona usługi polegające przede wszystkim na:

1. przygotowaniu koncepcji i harmonogramu wdrożenia systemu wraz odmiejszczeniem backupu,

W ramach przygotowania koncepcji wdrożenia systemu Wykonawca zobowiązuje się do:

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



- przeprowadzenia analizy przedwdrożeniowej, której celem jest zrozumienie specyficznych potrzeb i wymagań Zamawiającego,
- przeprowadzenia szczegółowego przeglądu aktualnego systemu backupu, w tym m. in.:
  - przedmiotu i metody wykonywania backupu,
  - harmonogramu i autoryzacji backupów,
  - zabezpieczenia dostępu do kopii,
  - monitorowania procesu oraz aktualizacji procedur,
  - oraz wszelkich związanych z tym komponentów, programów i usług,
- oceny aktualnej skuteczności i zgodności z najlepszymi praktykami w zakresie zabezpieczenia i odkładania danych,
- do uwzględnienia wykonania prac wdrożeniowych wymagających całkowitego wyłączenia dostępu do sieci w dni wolne od pracy Urzędu po wcześniejszym uzgodnieniu z Zamawiającym.

Wykonawca przedstawi po uwzględnieniu wymagań Zamawiającego do akceptacji opis architektury wybranego rozwiązania, w tym projekt wdrożenia systemu backupu, który musi zawierać co najmniej: opis funkcjonalny systemu, wykaz wymaganych elementów systemu, sposób ich wdrożenia i konfiguracji, szczegółowy opis architektury proponowanego rozwiązania wraz z opisem integracji z infrastrukturą techniczną Zamawiającego wraz z planem wdrożenia obejmującym harmonogram działań.

2. wykonanie wdrożenia, przy aktywnym udziale personelu Zamawiającego, na podstawie zaakceptowanej przez Zamawiającego koncepcji i harmonogramu, w tym:

- dostawy, instalacji i uruchomienia oferowanego sprzętu,
- instalacja agentów oprogramowania do wykonywania kopii zapasowych na serwerach i urządzeniach końcowych Zamawiającego,
- wdrożenie polityk usprawniających podłączanie nowego sprzętu Zamawiającego do systemu kopii zapasowych,
- połączenie wszystkich urządzeń Zamawiającego przewidzianych na etapie analizy do wdrażanego systemu,
- instalacja odmiejscowionego repozytorium zapasowego oraz jego konfiguracja w ramach spójnego systemu,
- zaaplikowanie zaplanowanych polityk wykonywania kopii zapasowych,
- wdrożenie musi zostać realizowane bezpośrednio przez producenta oferowanego systemu backupowego i przeprowadzone przez dedykowanego inżyniera od producenta systemu backupowego,
- wdrożenie powinno być zrealizowane tak, aby dostosować się do preferencji Zamawiającego.
- Zamawiający powinien móc skorzystać z przynajmniej 2h pomocy wdrożeniowej bezpośrednio świadczonej przez producenta rozwiązania.

3. przeprowadzenie testów po wdrożeniu w celu weryfikacji poprawności działania systemu oraz optymalizacja konfiguracji systemu na podstawie przeprowadzonych testów

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

4. przygotowanie dokumentacji powykonawczej:

Dokumentacja powykonawcza musi zawierać procedury administracyjne i operacyjne oraz inne informacje, istotne w eksploatacji systemu, w tym co najmniej:

- procedury i instrukcje dotyczące instalacji, konfiguracji i aktualizacji systemu,
- procedury dotyczące wykonywania i przechowywania kopii,
- instrukcje dla administratorów, w tym procedury zarządzania urządzeniami,
- inne niezbędne dokumenty, jakie powstaną w trakcie realizacji wdrożenia systemu, uzgodnione z przedstawicielami Zamawiającego.

Dokumentacja musi być przekazana w wersji elektronicznej i napisana w języku polskim. Procedury i instrukcje producenta mogą być przekazane w języku angielskim lub polskim.

Ad. 4 **Zarządzalne przełączniki sieciowe LAN**

**W ramach postępowania należy dostarczyć i wdrożyć 2 zestawy (TYP 1) i 1 zestaw (TYP 2).**

**Przełącznik TYP 1**

|    | <b>Minimalne wymaganie dotyczące jednej sztuki przełącznika dostępowego TYP1. W ramach postępowania należy dostarczyć 2 zestawy.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie Rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie Rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.                                                                                                                                                                                                                  |
| 2. | Wymagane parametry fizyczne:<br>a) możliwość montażu w stelażu/szafie 19"<br>b) wysokość maksymalna 1U<br>c) głębokość bez zainstalowanego zasilacza nie większa niż 36 cm<br>d) dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap).<br>e) zakres temperatur pracy ciągłej co najmniej od -5°C do +45°C<br>f) zakres wilgotności pracy co najmniej 5% - 94%<br>g) waga bez zainstalowanych modułów zasilania nie większa niż 5,7 kg |
| 3. | Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:<br>● 24 porty 100/1000BASE-T<br>● 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC<br>Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.                                                                                                                                                                                                                                                                                                        |
| 4. | Przełącznik musi posiadać następujące porty służące do zarządzania:<br>● Port konsoli ze złączem RJ45                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5.  | Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:<br>a) Zarządzanie stosem poprzez jeden adres IP<br>b) Do min. 9 jednostek w stosie<br>c) Porty do stackowania mogą być współdzielone z portami typu uplink.<br>d) Magistrala stackująca o wydajności minimum 80Gb/s<br>e) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)<br>f) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree<br>g) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.<br>h) W stosie musi być możliwość budowania pomiędzy przełącznikami: TYP1 i TYP2.<br>i) Zamawiający wymaga, aby z każdym zestawem był dostarczony oryginalny kabel producenta do stackowania SFP+ 10G o długości min. 60 cm. |
| 6.  | Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 7.  | Obsługa min. 32 500 adresów MAC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 8.  | Wbudowana pamięć RAM min. 1GB.<br>Minimalne taktowanie procesora 1000MHz<br>Bufor pakietów minimum: 2MB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 9.  | Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 10. | Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 11. | Możliwość skonfigurowania min. 1020 interfejsów vlan interface SVI działających równocześnie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 12. | Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 13. | Obsługa minimum 125 grup LAG                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 14. | Obsługa ramek jumbo o wielkości min. 12216 bajtów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 15. | Obsługa sFlow                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 16. | Wsparcie dla G.8032 ERPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 17. | Obsługa protokołu VRRP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 18. | Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).<br>Wsparcie dla mechanizmu PVST+ lub równoważnego.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 19. | Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP.<br>Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 20. | Obsługa min. 12 000 tras dla routingu IPv4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 21. | Obsługa min. 4 000 tras dla routingu IPv6<br>Obsługa min. 4 000 IPv6 neighbor discovery (ND)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 22. | Obsługa protokołów związanych z obsługą ruchu typu multicast:<br>a) IGMP v3<br>b) IGMP Snooping v3<br>c) PIM-SM, PIM-SSM i PIM-DM<br>d) MSDP i MLD Snooping<br>e) minimum 4000 tras multicast dla IPv4 i minimum 2000 tras multicast dla IPv6                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 23. | Minimalny rozmiar tablicy ARP 8 000 wpisów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 24. | Obsługa protokołów LLDP i LLDP-MED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 25. | Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 26. | <p>Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:</p> <ul style="list-style-type: none"> <li>a) min. 3 poziomy dostęp administracyjny poprzez konsolę</li> <li>b) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz przypisania listy ACL</li> <li>c) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC</li> <li>d) obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1900 reguł ACL</li> <li>e) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2</li> <li>f) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP</li> <li>g) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard</li> <li>h) możliwość synchronizacji czasu zgodnie z NTP lub SNTP</li> </ul> |
| 27. | <p>Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:</p> <ul style="list-style-type: none"> <li>● klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP</li> <li>● wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ</li> </ul>                                                                                                                                                                                                                                                                |
| 28. | Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).<br>Obsługa mechanizmu RSPAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 29. | <p>Wymagane opcje zarządzania:</p> <ul style="list-style-type: none"> <li>a) możliwość lokalnej obserwacji ruchu na określonym porcie</li> <li>b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)</li> <li>c) wsparcie dla skryptów python uruchamianych na urządzeniu</li> <li>d) wsparcie dla RMON</li> </ul>                                                                                                                                                                                                                                                                                                                                                          |
| 30. | <p>Wraz z urządzeniami muszą zostać dostarczone:</p> <ul style="list-style-type: none"> <li>a) pełna dokumentacja w języku polskim lub angielskim</li> <li>b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 31. | Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 32. | Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 33. | Zamawiający wymaga, aby przełączniki posiadały minimum 12 miesięczny serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | <p>Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).</p> <p>W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 34. | <p>Wraz z urządzeniem należy dostarczyć system centralnego zarządzania pochodzący od producenta oferowanych urządzeń.</p> <p>System centralnego zarządzania może być dostarczony w formie:</p> <ol style="list-style-type: none"> <li>1) Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej. Usługa musi być świadczona minimum przez okres serwisu gwarancyjnego urządzenia</li> <li>lub</li> <li>2) Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.</li> </ol> <p>Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.</p> <p>W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.</p> <p>System centralnego zarządzania musi umożliwiać:</p> <ul style="list-style-type: none"> <li>- tworzenie VLANów</li> <li>- ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu</li> <li>- tworzenie połączeń zagregowanych</li> <li>- monitorowanie statusu pracy przełącznika i portów</li> <li>- możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania</li> <li>- możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego</li> </ul> |
| 35. | <p>Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Przełącznik TYP 2

|     |                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | <p><b>Minimalne wymaganie dotyczące jednej sztuki przełącznika dostępowego TYP2. W ramach postępowania należy dostarczyć 1 zestaw</b></p>                                                                                                                                                                                                                                                                 |
| 36. | <p>Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie Rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie Rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej.</p> |
| 37. | <p>Wymagane parametry fizyczne:</p>                                                                                                                                                                                                                                                                                                                                                                       |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | <p>h) możliwość montażu w stelażu/szafie 19"</p> <p>i) wysokość maksymalna 1U</p> <p>j) głębokość bez zainstalowanego zasilacza nie większa niż 40 cm</p> <p>k) dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Każde urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap)</p> <p>l) zakres temperatur pracy ciągłej co najmniej od -5°C do +45 °C</p> <p>m) zakres wilgotności pracy co najmniej 5% - 94%</p> <p>n) waga bez zainstalowanych modułów zasilania nie większa niż 7,6 kg</p>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 38. | <p>Przełącznik musi zostać dostarczony z następującymi interfejsami Ethernet mogącymi działać równocześnie:</p> <ul style="list-style-type: none"> <li>● 24 porty 100/1000BASE-T zgodne ze standardem 802.3at (minimalny budżet mocy PoE: 1100W)</li> <li>● 4 porty 10GE SFP+ z obsługą modułów 10G-SR, 10G-LR, 1G-SX, 1G-LX, 1GBase-T (RJ45), kabli DAC</li> </ul> <p>Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 39. | <p>Przełącznik musi posiadać następujące porty służące do zarządzania:</p> <ul style="list-style-type: none"> <li>● Port konsoli ze złączem RJ45</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 40. | <p>Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:</p> <p>j) Zarządzanie stosem poprzez jeden adres IP</p> <p>k) Do min. 9 jednostek w stosie</p> <p>l) Porty do stackowania mogą być współdzielone z portami typu uplink.</p> <p>m) Magistrala stackująca o wydajności minimum 80Gb/s</p> <p>n) Możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation)</p> <p>o) Stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree</p> <p>p) Jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.</p> <p>q) W stosie musi być możliwość budowania pomiędzy przełącznikami: TYP1 i TYP2.</p> <p>r) Zamawiający wymaga, aby z każdym zestawem był dostarczony oryginalny kabel producenta do stackowania SFP+ 10G o długości min. 60 cm.</p> |
| 41. | Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 95 Mpps                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 42. | Obsługa min. 32 500 adresów MAC                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 43. | <p>Wbudowana pamięć RAM min. 1GB.</p> <p>Minimalne taktowanie procesora 1000MHz</p> <p>Bufor pakietów minimum: 2MB</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 44. | Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512MB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 45. | Obsługa min. 4090 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 46. | Możliwość skonfigurowania min. 1020 interfejsów vlan interface SVI działających równocześnie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 47. | Możliwość tworzenie połączeń agregowanych (link aggregation) zgodnych ze standardem 802.3ad                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 48. | Obsługa minimum 125 grup LAG                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 49. | Obsługa ramek jumbo o wielkości min. 12216 bajtów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 50. | Obsługa sFlow                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 51. | Wsparcie dla G.8032 ERPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 52. | Obsługa protokołu VRRP                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 53. | Wsparcie dla protokołów 802.1d (STP), 802.1s (MSTP), 802.1w (RSTP).<br>Wsparcie dla mechanizmu PVST+ lub równoważnego                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 54. | Obsługa protokołów routingu dynamicznego OSPF, OSPFv3, RIP, RIPng, IS-IS, BGP. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 55. | Obsługa min. 12 000 tras dla routingu IPv4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 56. | Obsługa min. 4 000 tras dla routingu IPv6<br>Obsługa min. 4 000 IPv6 neighbor discovery (ND)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 57. | Obsługa protokołów związanych z obsługą ruchu typu multicast:<br>a) IGMP v3<br>b) IGMP Snooping v3<br>c) PIM-SM, PIM-SSM i PIM-DM<br>d) MSDP i MLD Snooping<br>e) minimum 4000 tras multicast dla IPv4 i minimum 2000 tras multicast dla IPv6                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 58. | Minimalny rozmiar tablicy ARP 8 000 wpisów                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 59. | Obsługa protokołów LLDP i LLDP-MED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 60. | Przełącznik musi posiadać funkcjonalność DHCP Server, DHCP Snooping, DHCP relay, DHCP client                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 61. | Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:<br>i) min. 3 poziomy dostępu administracyjnego poprzez konsolę<br>j) autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz przypisania listy ACL<br>k) możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC<br>l) obsługa sprzętowo reguł ACL. Możliwość utworzenia minimum 1900 reguł ACL<br>m) zarządzanie urządzeniem z wykorzystaniem HTTPS, SNMPv3 (IPv4 i IPv6) i SSHv2<br>n) możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP<br>o) obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard<br>p) możliwość synchronizacji czasu zgodnie z NTP lub SNTP |
| 62. | Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:<br><ul style="list-style-type: none"> <li>• klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP</li> <li>• wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR, WFQ</li> </ul>                                                                                                                                                                       |
| 63. | Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA).<br>Obsługa mechanizmu RSPAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 64. | Wymagane opcje zarządzania:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | <ul style="list-style-type: none"> <li>a) możliwość lokalnej obserwacji ruchu na określonym porcie</li> <li>b) plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC)</li> <li>c) wsparcie dla skryptów python uruchamianych na urządzeniu</li> <li>d) wsparcie dla RMON</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 65. | <p>Wraz z urządzeniami muszą zostać dostarczone:</p> <ul style="list-style-type: none"> <li>a) pełna dokumentacja w języku polskim lub angielskim</li> <li>b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 66. | <p>Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 67. | <p>Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 68. | <p>Zamawiający wymaga, aby przełączniki posiadały minimum 12 miesięczny serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń</p> <p>Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Do odbioru końcowego przedmiotu umowy Wykonawca przedłoży oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).</p> <p>W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.</p>                                                                                                                                                                                                                                                                                                                 |
| 69. | <p>Wraz z urządzeniem należy dostarczyć system centralnego zarządzania pochodzący od producenta oferowanych urządzeń.</p> <p>System centralnego zarządzania może być dostarczony w formie:</p> <ul style="list-style-type: none"> <li>1) Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej. Usługa musi być świadczona minimum przez okres serwisu gwarancyjnego urządzenia</li> <li>Lub</li> <li>2) Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.</li> </ul> <p>Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.</p> <p>W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.</p> |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | System centralnego zarządzania musi umożliwiać:<br>- tworzenie VLANów<br>- ustawianie trybu pracy danego portu (access/trunk) z dodaniem odpowiedniego VLANu<br>- tworzenie połączeń zagregowanych<br>- monitorowanie statusu pracy przełącznika i portów<br>- możliwość uruchomienia CLI przełącznika w panelu systemu do zarządzania<br>- możliwość wykonania aktualizacji oprogramowania dla danego przełącznika sieciowego |
| 70. | Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń.                                                                                                                                                                                                                                                                                               |

**Ad. 5 Punkty dostępne sieci bezprzewodowej WiFi.**

**W ramach zadania należy dostarczyć i wdrożyć 2 zestawy.**

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>Minimalne wymagania dotyczące punktu dostępowego.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 1. | Punkt dostępowy musi być dedykowanym urządzeniem sieciowym przystosowanym do zamontowania na suficie i na ścianie. Wymagane dostarczenie z zestawu montażowego. System operacyjny (firmware) musi być dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej. Oprogramowanie do pracy w trybie tzw „lekkiego AP”, możliwość pracy jako tzw. „grubego AP (FAT AP)” oraz możliwość pracy jako tzw. Kontroler AP, czyli jeden z punktów dostępowych musi mieć możliwość pracy jako kontroler WLAN.                                                                      |
| 2. | Urządzenie w trybie FAT musi umożliwiać zarządzać pracą dodatkowych access-pointów tego samego producenta. Funkcjonalność zarządzania pracą pozostałymi access-pointami musi umożliwiać transfer ruchu w trybie „local forwarding” (ruch z każdego access-pointa przesyłany jest bezpośrednio w sieci lokalnej) oraz „Gateway” (access-point w trybie FAT działa jako brama sieci dla pozostałych access-pointów, realizując m.in. funkcjonalność NAT). Funkcjonalność zarządzania pracą pozostałymi urządzeniami musi być realizowana z poziomu przeglądarki urządzenia FAT, jak również z poziomu CLI (z wykorzystaniem m.in. protokołu SSH) urządzenia FAT |
| 3. | Wymagane parametry fizyczne:<br>a) możliwość montażu na suficie oraz ścianie (wraz z urządzeniem należy dostarczyć elementy to montowania)<br>b) wysokość maksymalna 5 cm<br>c) możliwość zasilania przez zasilacz DC<br>d) zakres temperatur pracy ciągłej co najmniej 0°C – +45°C<br>e) zakres wilgotności pracy co najmniej 5% - 95%                                                                                                                                                                                                                                                                                                                       |
| 4. | Punkt dostępowy musi posiadać:<br>a) dedykowany port konsolowy<br>b) minimum 1 port 100/1000Mbit Base-T PoE                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 5. | Obsługiwane standardy radiowe: 802.11a/b/g/n/ac/ac Wave 2/11ax, jednoczesna obsługa minimum 16 SSID dla każdego radia                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 6. | Wbudowane anteny minimum 4dBi dla 2,4GHz oraz 6dBi dla 5GHz z pracą w standardzie minimum MIMO: 2.4G: 2x2, 5G: 2x2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.  | Wsparcie dla standardów/funkcjonalności bezpieczeństwa: WPA, WPA2, WPA3, 802.1x, IP Source Guard (IPSG) oraz tworzenie ACL                                                                                                                                                                                                                     |
| 8.  | Wsparcie dla roamingu zgodnego z 802.11k, 802.11v, 802.11r                                                                                                                                                                                                                                                                                     |
| 9.  | Obsługa minimum 1000 równocześnie podłączonych użytkowników do punktu dostępowego                                                                                                                                                                                                                                                              |
| 10. | Wydajność minimum 1,7Gbps w tym minimum 500Mbps dla 2.4GHz oraz 1,2Gbps dla 5GHz                                                                                                                                                                                                                                                               |
| 11. | Obsługa BLE w wersji 5.0                                                                                                                                                                                                                                                                                                                       |
| 12. | Zużycie mocy nie większe niż 14W                                                                                                                                                                                                                                                                                                               |
| 13. | Możliwość zarządzania poprzez: <ul style="list-style-type: none"> <li>a) WWW over HTTPS</li> <li>b) kontroler tego samego producenta</li> <li>c) SNMP v1, v2c, v3,</li> <li>d) Dedykowany port konsoli</li> <li>e) SSHv2</li> </ul>                                                                                                            |
| 14. | Kompatybilność dla protokołów oraz standardów sieciowych takich jak: IPv6, LLDP, mDNS, NAT, IPsec                                                                                                                                                                                                                                              |
| 15. | Urządzenie musi posiadać standard bezpieczeństwa EN62368-1                                                                                                                                                                                                                                                                                     |
| 16. | Tunel CAPWAP dla komunikacji z kontrolerem muszą być zaszyfrowane celem ochrony przed możliwością podsłuchania transmisji w sieci kablowej                                                                                                                                                                                                     |
| 17. | Wsparcie dla protokołów i standardów: <ul style="list-style-type: none"> <li>a) 802.11e</li> <li>b) 802.11i</li> <li>c) 802.11d</li> <li>d) 802.11h</li> <li>e) 802.11u</li> <li>f) 802.11w</li> <li>g) 802.15.1</li> <li>h) LLDP</li> <li>i) MLD Snooping i IGMP Snooping</li> <li>j) DTLS encryption</li> <li>k) A-MPDU i A-MSDU</li> </ul>  |
| 18. | Obsługa NTP lub SNTP                                                                                                                                                                                                                                                                                                                           |
| 19. | Wraz z urządzeniami muszą zostać dostarczone: <ul style="list-style-type: none"> <li>a) pełna dokumentacja w języku polskim lub angielskim</li> <li>b) dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana</li> </ul> |
| 20. | Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich                                                                                               |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | poprawnej pracy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 21. | Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 22. | Zamawiający wymaga, aby urządzenia posiadały min. 12 miesięczny serwis gwarancyjny świadczony przez producenta lub Wykonawcę (lub autoryzowany serwis) na bazie wsparcia serwisowego wykupionego u producenta oferowanych urządzeń<br>Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia. Zamawiający na etapie dostawy będzie wymagał oświadczenia producenta potwierdzającego nabycie oraz zarejestrowanie serwisu gwarancyjnego na Zamawiającego. Wszystkie koszty związane z naprawami gwarancyjnymi nie mogą obciążać Zamawiającego (np. koszty wysyłki).<br>W celu zapewnienia odpowiedniego poziomu świadczonych usług Wykonawca/autoryzowany serwis producenta musi posiadać status autoryzowanego partnera serwisowego przyznawany przez producenta dla oferowanych urządzeń, a usługa serwisu musi być świadczona w języku polskim.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 23. | Wraz z urządzeniem należy dostarczyć system centralnego zarządzania pochodzący od producenta oferowanych urządzeń.<br>System centralnego zarządzania może być dostarczony w formie:<br>1. Usługi w Internecie, świadczonej przez producenta sprzętu, na serwerach zlokalizowanych w Unii Europejskiej<br>Lub<br>2. Dedykowanego oprogramowania wraz dostawą dedykowanej platformy sprzętowej, do zainstalowania w środowisku Zamawiającego.<br>Jeżeli dostęp do systemu centralnego zarządzania wymaga licencji to w ramach postępowania należy dostarczyć odpowiednie licencje umożliwiające korzystanie z systemu centralnego zarządzania minimum przez okres serwisu gwarancyjnego.<br>W przypadku dostarczenia dedykowanego oprogramowania instalowanego w środowisku Zamawiającego, Wykonawca zobowiązany jest dostarczyć niezbędną platformę sprzętową. Dostarczona platforma musi być nowa i nieużywana wcześniej w żadnych projektach oraz musi objęta wsparciem serwisowym producenta minimum przez okres trwania gwarancji serwisowej dla oferowanych urządzeń sieciowych.<br>System centralnego zarządzania musi umożliwiać:<br>- tworzenie VLANów<br>- tworzenie SSID dla sieci WiFi z możliwością przypisania VLANu<br>- tworzenie zabezpieczeń dla SSID<br>- monitorowanie statusu pracy punktów dostępowych<br>- możliwość uruchomienia CLI w panelu systemu do zarządzania<br>- możliwość wykonania aktualizacji oprogramowania dla danego punktu dostępowego |
| 24. | Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres gwarancji urządzenia.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Przełączniki sieciowe LAN i punkty dostępowe Wifi muszą pochodzić od tego samego producenta w celu zapewnienia spójnego zarządzania z poziomu wspólnego interfejsu.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



W ramach zadania Wykonawca:

- a) wykona inwentaryzację sprzętu aktywnego w serwerowni Zamawiającego;
- b) przeorganizuje wyposażenie konstrukcji stelażowej Rack znajdującej się w serwerowni w celu montażu nowych urządzeń, włącznie z uporządkowaniem okablowania LAN wchodzącego do Rack poprzez montaż nowych patchpaneli z wyposażeniem zgodnym z istniejącym okablowaniem LAN i zaterminowanie istniejących kabli na modułach Keystone RJ-45;
- c) dostarczy nowe patchcordsy i wykrośnie wszystkich użytkowników i urządzenia;
- d) zdemontuje niepotrzebny sprzęt i protokolarnie przekaze go użytkownikowi.

**Ad. 6 Zasilacze UPS dla stacji komputerowych (należy dostarczyć 25 szt.)**

Minimalne parametry

| PARAMETR                                                | CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Minimalne wymagania techniczne dla jednostki UPS</i> | <p>Moc znamionowa jednostki nie mniej niż 480W / 900VA</p> <p>Topologia line-interactive</p> <p>Temperatura eksploatacji 0 - 40 °C</p> <ul style="list-style-type: none"> <li>• Wilgotność względna podczas pracy 0 - 95 %</li> <li>• Wysokość n.p.m. podczas pracy 0-3000 m</li> <li>• Klasa energetyczna sprzętu przeciwprzepięciowego 273 Dżule</li> <li>• Zabezpieczenie przeciwprzepięciowe: bezpiecznik minimum 7A</li> </ul>                           |
| <i>Parametry wejściowe</i>                              | <ul style="list-style-type: none"> <li>• Nominalne napięcie wejściowe 230V</li> <li>• Częstotliwość wejściowa 50/60 Hz (automatyczne wykrywanie)</li> <li>• Standard wtyczki: Schuko CEE 7/7P</li> </ul>                                                                                                                                                                                                                                                      |
| <i>Parametry wyjściowe</i>                              | <ul style="list-style-type: none"> <li>• Napięcie wyjściowe 230V</li> <li>• Zniekształcenia napięcia wyjściowego +/- 10%</li> <li>• Częstotliwość na wyjściu przy pracy bateryjnej 50/60Hz +/- 0.5Hz</li> <li>• Współczynnik mocy: minimum 0.53</li> <li>• Typ przebiegu: Schodkowa aproksymacja sinusoidy</li> <li>• Złącza/gniazda wyjściowe: 2 gniazda Schuko z zabezpieczeniem przeciwprzepięciowym oraz podtrzymaniem zasilania.</li> </ul>              |
| <i>Akumulatory i czas podtrzymania</i>                  | <ul style="list-style-type: none"> <li>• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu</li> <li>• Czas autonomii: <ul style="list-style-type: none"> <li>1 minuta dla pełnego obciążenia</li> <li>6 minut 30 sekund dla połowy obciążenia</li> </ul> </li> <li>• Typowy czas ładowania 8 godzin</li> <li>• Oczekiwana żywotność akumulatora (lata) 3 – 5</li> <li>• Baterie wymieniane na gorąco</li> </ul> |
| <i>Komunikacja i zarządzanie</i>                        | <ul style="list-style-type: none"> <li>• Diody LED wskazująca na status zasilania: zasilanie z sieci energetycznej: zasilanie z akumulatora</li> <li>• Alarm dźwiękowy: Praca na baterii, niski poziom naładowania baterii, wyłączenie baterii, zastępcza bateria wykryta</li> </ul>                                                                                                                                                                          |
| <i>Certyfikaty, zgodności oraz</i>                      | <ul style="list-style-type: none"> <li>• Znak C, CE, RoHS, REACH</li> <li>• Min. 12 miesięcy na naprawę lub wymianę</li> </ul>                                                                                                                                                                                                                                                                                                                                |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



|           |  |
|-----------|--|
| gwarancja |  |
|-----------|--|

**Ad. 7 Zasilacze UPS dla sprzętu serwerowego (należy dostarczyć 3 szt.)**

Minimalne parametry

| PARAMETR                                                | CECHA/WARTOŚĆ/WŁAŚCIWOŚĆ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Minimalne wymagania techniczne dla jednostki UPS</i> | <p>Moc znamionowa jednostki nie mniej niż 1800W / 2000VA</p> <p>Obudowa typu Tower</p> <p>Technologia Double Conversion (On-Line)</p> <p>Temperatura eksploatacji 0 - 40 °C</p> <ul style="list-style-type: none"> <li>• Wilgotność względna podczas pracy 0 - 95 %</li> <li>• Wysokość n.p.m. podczas pracy 0-2000m, powyżej 2000m n. p. m. następuje obniżenie wartości znamionowych</li> <li>• Klasa energetyczna sprzętu przeciwprzepięciowego 945 Dżuli</li> <li>• Możliwość zimnego startu</li> <li>• Automatyczne włączenie UPS-a po powrocie zasilania</li> </ul> |
| <i>Parametry wejściowe</i>                              | <ul style="list-style-type: none"> <li>• Nominalne napięcie wejściowe 220V, 230V, 240V</li> <li>• Zakres częstotliwości wejściowej: 40-70 Hz</li> <li>• Typ gniazda wejściowego: IEC-320 C14</li> <li>• Zmienny zakres napięcia wejściowego w trybie podstawowym 110-285V</li> </ul>                                                                                                                                                                                                                                                                                      |
| <i>Parametry wyjściowe</i>                              | <ul style="list-style-type: none"> <li>• Napięcie wyjściowe 220V, 230V, 240V</li> <li>• Zniekształcenia napięcia poniżej 3% dla obciążeń liniowych oraz poniżej 6% dla obciążeń nieliniowych</li> <li>• Częstotliwość na wyjściu zsynchronizowana z siecią zasilającą 50/60 Hz (<math>\pm 3</math>Hz dla zasilania z sieci lub <math>\pm 0.1</math>Hz dla zasilania z baterii)</li> <li>• Typ przebiegu sinusoida</li> <li>• Złącza/gniazda wyjściowe 4 szt. IEC 320 C13</li> </ul>                                                                                       |
| <i>Akumulatory i czas podtrzymania</i>                  | <ul style="list-style-type: none"> <li>• Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu</li> <li>• Czas autonomii pracy przy zasilaniu akumulatorowym: 3 minuty 4 sekundy dla pełnego obciążenia 10 minut 53 sekundy dla połowy obciążenia</li> <li>• Typowy czas ładowania 4 godziny</li> <li>• Oczekiwana żywotność akumulatora (lata) 3 – 5</li> <li>• Automatyczny test akumulatora</li> </ul>                                                                                                                       |
| <i>Komunikacja i zarządzanie</i>                        | <ul style="list-style-type: none"> <li>• Porty komunikacyjne: RS-232 Serial, USB, Smart Slot (karta zarządzania sieciowego SNMP sprzedawana oddzielnie)</li> <li>• Panel sterowania: Wielofunkcyjna konsola sterownicza i informacyjna LCD</li> </ul> <p>Alarm dźwiękowy: Alarm przy zasilaniu z akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia</p> <ul style="list-style-type: none"> <li>• Złącze awaryjnego wyłączenia zasilania (EPO)</li> </ul>                                                                   |
| <i>Certyfikaty, zgodności oraz</i>                      | <ul style="list-style-type: none"> <li>• Znak CE, RoHS, REACH</li> <li>• Min. 12 miesięcy na naprawę lub wymianę</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



|                       |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>gwarancja</i>      |                                                                                                                                                                                                                                                                                                                                                                                                 |
| <i>Oprogramowanie</i> | <ul style="list-style-type: none"><li>• Dostępne oprogramowanie do zarządzania/monitoringu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®.</li></ul> |

**Ad. 8 Urządzenia UTM w Publicznej Szkole Podstawowej w Lubichowie im. Ks. Kard. Stefana Wyszyńskiego oraz Publicznej Szkole Podstawowej w Zelgoszczy**

(TYP 1 i TYP 2)

W ramach zadania należy dostarczyć i skonfigurować 2 urządzenia UTM (1 szt. TYP1 + 1 szt. TYP2) w Publicznej Szkole Podstawowej w Lubichowie im. Ks. Kard. Stefana Wyszyńskiego oraz 1 urządzenie TYP2 w Publicznej Szkole Podstawowej w Zelgoszczy.

**Wymagania minimalne wspólne dla TYP 1 i TYP 2.**

**OBSŁUGA SIECI**

1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.

**ZAPORA KORPORACYJNA (Firewall)**

1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.
2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.
3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
4. Interfejs (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

#### **INTRUSION PREVENTION SYSTEM (IPS)**

1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
9. Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
10. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

#### **KSZTAŁTOWANIE PASMA (Traffic Shapping)**

1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
3. Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

#### **OCHRONA ANTYWIRUSOWA**

1. Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

#### OCHRONA ANTYSKAM

1. Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
2. Ochrona antyskam ma działać w oparciu o:
  - a. białe/czarne listy,
  - b. DNS RBL,
  - c. Skaner heurystyczny.
3. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.

#### WIRTUALNE SIECI PRYWATNE (VPN)

1. Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
2. Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
  - a. PPTP VPN,
  - b. IPSec VPN,
  - c. SSL VPN.
3. SSL VPN ma działać co najmniej w trybach tunelu i portalu.
4. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
5. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
6. Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
7. Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.
8. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

#### FILTR DOSTĘPU DO STRON WWW

1. Urządzenie ma posiadać wbudowany filtr URL.
2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
3. Administrator ma mieć możliwość dodawania własnych kategorii URL.
4. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
  - a. blokowanie dostępu do adresu URL,
  - b. zezwolenie na dostęp do adresu URL,
  - c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
5. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



6. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
7. Filtr URL musi uwzględniać komunikację po protokole HTTPS.
8. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
9. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

#### UWIERZYTELNIANIE

1. Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
  - a. lokalną bazę użytkowników (wewnętrzny LDAP),
  - b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),
  - c. usługę katalogową Microsoft Active Directory.
2. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
3. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
  - a. SSL,
  - b. Radius,
  - c. Kerberos.
4. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
5. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
6. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
7. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
8. Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
9. Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPsec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.

#### ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)

1. Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
2. Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:
  - a. równoważenie względem adresu źródłowego,
  - b. równoważenie względem połączenia.
3. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.
4. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



5. Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
6. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).
7. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

#### ROUTING (TRASOWANIE)

1. Urządzenie ma umożliwiać statyczne trasowanie pakietów.
2. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
3. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
4. Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

#### ADMINISTRACJA URZĄDZENIEM

1. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
2. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
6. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH)
7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording ).
13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.
15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
  - a. manualnego eksportu do pliku w dowolnym momencie czasu,
  - b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

## RAPORTOWANIE

1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

## POZOSTAŁE USŁUGI I FUNKCJE

1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
2. Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
3. Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
4. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
5. Urządzenie ma posiadać usługę DNS Proxy.
6. Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
7. Urządzenie musi mieć zaimplementowane Open API
8. Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



- ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
9. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
  10. Urządzenie musi oferować możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.

#### **GWARANCJA I SERWIS**

1. Urządzenie ma być objęte minimum 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. Okres gwarancji liczony
2. od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia
3. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.

#### **PARAMETRY SPRZĘTOWE (TYP 1)**

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci Flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
3. Liczba portów Ethernet 2,5Gbps – min. 8.
4. Liczba portów światłowodowych 1Gbps – min. 1.
5. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
6. Przepustowość Firewall (1518 bajtów UDP) – minimum 4Gbps.
7. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 2Gbps.
8. Przepustowość filtrowania Antywirusowego – minimum 500Mbps.
9. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
10. Maksymalna liczba tuneli VPN IPSec – minimum 100.
11. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 50.
12. Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 50.
13. Obsługa interfejsów 802.11q (VLAN) – minimum 128
14. Liczba równoczesnych sesji – minimum 300 000 i nie mniej niż 20 000 nowych sesji/sekundę.
15. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
16. Urządzenie nie ma limitu na liczbę użytkowników.
17. Liczba reguł filtrowania – minimum 8 192.
18. Liczba tras statycznego routingu – minimum 512.
19. Liczba tras dynamicznego routingu – minimum 10 000.
20. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia.
21. Urządzenie musi być wyposażone w moduł TPM.

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



## **PARAMETRY SPRZĘTOWE (TYP 2)**

1. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci Flash.
2. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD.
3. Liczba portów Ethernet 2,5Gbps – min.4.
4. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
5. Przepustowość Firewall (1518 bajtów UDP) – minimum 3Gbps.
6. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 1Gbps.
7. Przepustowość filtrowania Antywirusowego – minimum 300Mbps.
8. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 1Gbps.
9. Maksymalna liczba tuneli VPN IPSec – minimum 50.
10. Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 25.
11. Obsługa interfejsów 802.11q (VLAN) – minimum 128
12. Liczba równoczesnych sesji – minimum 150 000 i nie mniej niż 15 000 nowych sesji/sekundę.
13. Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
14. Urządzenie nie ma limitu na liczbę użytkowników.
15. Liczba reguł filtrowania – minimum 1024.
16. Liczba tras statycznego routingu – minimum 512.
17. Liczba tras dynamicznego routingu – minimum 10 000.
18. Urządzenie musi posiadać pasywny system chłodzenia.
19. Urządzenie ma być przystosowane do pracy w temperaturach od -20oC do +60oC przy wilgotności od 0% do 95% (bez kondensacji).

## **Ad. 9 Platforma szkoleniowa.**

Przedmiotem oferty jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa” (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej dla 40 osób z zakresu podstaw bezpieczeństwa w Internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy.

Usługa musi zawierać:

1. Platformę szkoleniową zawierającą min. 45 szkoleń, dostępnych w języku polskim (oraz w jęz. angielskim, niemieckim, hiszpańskim, czeskim, słowackim, serbskim, chorwackim i włoskim), w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.

a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- Podstawy bezpiecznego Internetu
- Bezpieczeństwo poczty
- Załączniki w poczcie elektronicznej
- Phishing
- Spyware/malware
- Bezpieczeństwo danych osobowych RODO/GDRP
- Bezpieczne hasła

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



- Managery haseł
- Bezpieczeństwo urządzeń mobilnych
- Uwierzytelnianie wieloskładnikowe (MFA)
- Bezpieczna praca zdalna
- Bezpieczna praca w biurze
- Sieci społeczne
- Socjotechnika stosowana
- Zakupy w Internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.

c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić min. 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

- a) z linkiem prowadzącym do stronnym internetowej,
- b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
- c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
- d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. dedykowaną platformę dostarczającą raporty obejmujące minimum:

- a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
- b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zawierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 10 zmian w okresie trwania usługi).
- przeprowadzić minimum 5 kampanii phishingowych

**ZPP.271.2.2.2025 Specyfikacja Warunków Zamówienia**  
**Dostawa oprogramowania i sprzętu komputerowego wraz z usługą wdrożenia**



Fundusze Europejskie  
na Rozwój Cyfrowy



Rzeczpospolita  
Polska

Dofinansowane przez  
Unię Europejską



CENTRUM  
PROJEKTÓW  
POLSKA  
CYFROWA

Wymagania dodatkowe:

Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi. Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.

Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci Internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.

Do odbioru końcowego przedmiotu umowy Wykonawca przedłoży oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

**Ad. 10 Specjalistyczne szkolenia z zakresu cyberbezpieczeństwa IT.**

Wymagania na specjalistyczne szkolenia zostały określone każdorazowo przy pozycjach sprzętowo-programowych, których dotyczą.